(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号
特開2005-5821
(P2005-5821A)

(43)公開日 平成17年1月6日(2005.1.6)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601C	5B085
G06F 15/00	G06F	15/00	330C	5J104
	H04L	9/00	601E	

審査請求 未請求 請求項の数 12 OL （全 16 頁）

(21)出願番号 特願2003-164516(P2003-164516)
(22)出願日 平成15年6月10日(2003.6.10)

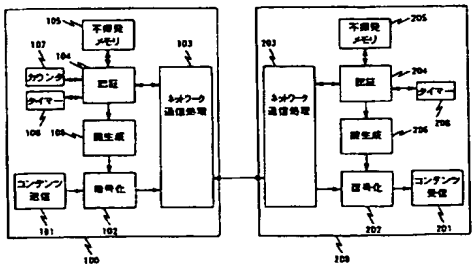
(71)出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人 100075096
弁理士 作田 康夫
(72)発明者 工藤 善道
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所デジタルメディア開発本部内
(72)発明者 佐々本 学
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所デジタルメディア開発本部内

最終頁に続く

(54)【発明の名称】コンテンツ送信装置、コンテンツ受信装置およびコンテンツ伝送方法

(57)【要約】
【課題】ＬＡＮを用いてコンテンツの伝送を行う際に不正なコピーの作成を抑止して著作権の保護を図ると共に、コンテンツ伝送を個人の使用の範囲を逸脱しないようにする。
【解決手段】コンテンツ送信装置とコンテンツ受信装置はコンテンツの伝送を行うのに先立ち相互認証を行い、互いがコンテンツを著作権を尊重して正当に扱う機器であることを確認した後に、共有化した鍵データによってコンテンツを暗号化して伝送する。認証の際には認証要求もしくは認証応答の送信に対する受信確認データの到来までの時間を計測して、この値が一定の上限値を超えないような場合に限ってコンテンツの伝送を行うようにする。これにより、認証されたコンテンツ受信装置以外の装置によってコンテンツが受信されて不正なコピーが作成されるのを防ぐと共に、コンテンツの送信が広域ネットワークなどを越えて行なわれるのを防ぐことができる。
【選択図】 図１

図 1



【特許請求の範囲】
【請求項１】
ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該ネットワークを介して接続されるコンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、
該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、
該認証手段で認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、
該コンテンツ受信装置への認証要求の送信もしくは該コンテンツ受信装置からの認証要求に対する応答の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を計測するタイマー手段とを有し、
該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ送信装置。
【請求項２】
前記タイマー手段において計測した前記コンテンツ受信装置への認証要求の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間の計測結果が所定の値を超えた場合には、前記認証手段において該コンテンツ受信装置の認証を不成功と判定することを特徴とする請求項１記載のコンテンツ送信装置。
【請求項３】
ネットワークを介して接続されるコンテンツ受信装置にコンテンツを送信する際に、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、
該コンテンツ受信装置への認証要求の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を計測するタイマー手段とを有し、
該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ送信装置。
【請求項４】
ネットワークを介して接続されるコンテンツ受信装置にコンテンツを送信する際に、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、
該コンテンツ受信装置からの認証要求に対する応答の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を計測するタイマー手段とを有し、
該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ送信装置。
【請求項５】
ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該ネットワークを介して接続されるコンテンツ送信装置から受信するコンテンツを該ネットワーク通信手段から受け取るコンテンツ受信処理手段と、
該コンテンツ送信装置に認証要求を発行して送るとともに、該コンテンツ送信装置から受信した認証要求に対する認証の判定を行う認証手段と、
該認証手段で認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該コンテンツ送信装置から受信したコンテンツの暗号復号化処理を行う復号化手段と、
該コンテンツ送信装置への認証要求の送信もしくは該コンテンツ送信装置からの認証要求に対する応答の送信に対する該コンテンツ送信装置からの受信確認の到達までの時間を計測するタイマー手段とを有し、
該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ送信装置からのコンテンツ受信を行わないことを特徴とするコンテンツ受信装置。

【請求項６】
前記タイマー手段において計測した前記コンテンツ送信装置への認証要求の送信に対する該コンテンツ送信装置からの受信確認の到達までの時間の計測結果が所定の値を超えた場合には、前記認証手段において該コンテンツ送信装置の認証を不成功と判定することを特徴とする請求項５記載のコンテンツ受信装置。
【請求項７】
ネットワークを介して接続されるコンテンツ送信装置とコンテンツ受信装置との間のコンテンツ伝送方法であって、
該コンテンツ送信装置は、
該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証ステップと、
認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化ステップと、
該コンテンツ受信装置への認証要求の送信もしくは該コンテンツ受信装置からの認証要求に対する応答の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を計測するステップとを有し、
該コンテンツ受信装置は
該コンテンツ送信装置に認証要求を発行して送るとともに、該コンテンツ送信装置から受信した認証要求に対する認証の判定を行う認証ステップと、
認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該コンテンツ送信装置から受信したコンテンツの暗号復号化処理を行う復号化ステップと、
該コンテンツ送信装置への認証要求の送信もしくは該コンテンツ送信装置からの認証要求に対する応答の送信に対する該コンテンツ送信装置からの受信確認の到達までの時間を計測するステップとを有し、
該コンテンツ送信装置の計測結果もしくは該コンテンツ受信装置の計測結果が所定の値を超えた場合には、該コンテンツ送信装置から該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ伝送方法。
【請求項８】
ネットワークを介して接続されるコンテンツ受信装置にコンテンツを送信するコンテンツ送信装置におけるコンテンツ伝送方法であって、
コンテンツを送信する際に、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証ステップと、
該コンテンツ受信装置への認証要求の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を計測するステップとを有し、
計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ送信装置におけるコンテンツ伝送方法。
【請求項９】
ネットワークを介して接続されるコンテンツ受信装置にコンテンツを送信するコンテンツ送信装置におけるコンテンツ伝送方法であって、
コンテンツを送信する際に、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証ステップと、
該コンテンツ受信装置からの認証要求に対する応答の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を計測するステップとを有し、
該計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ送信装置におけるコンテンツ伝送方法。
【請求項１０】

ネットワークを介して接続される情報受信装置に情報を送信する際に、該情報受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該情報受信装置に対して自身の認証要求を発行する認証手段と、
該情報受信装置への認証要求の送信に対する該情報受信装置からの受信確認の到達までの時間を計測する時間計測手段とを有し、
該時間計測手段での計測結果が所定の値を超えた場合には、該情報受信装置への情報送出を行わないことを特徴とする情報送信装置。
【請求項１１】
ネットワークを介して接続される情報受信装置に情報を送信する際に、該情報受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該情報受信装置に対して自身の認証要求を発行する認証手段と、
該情報受信装置からの認証要求に対する応答の送信に対する該情報受信装置からの受信確認の到達までの時間を計測する時間計測手段とを有し、
該時間計測手段での計測結果が所定の値を超えた場合には、該情報受信装置への情報送出を行わないことを特徴とする情報送信装置。
【請求項１２】
ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該ネットワークを介して接続される情報送信装置から受信する情報を該ネットワーク通信手段から受け取る情報受信処理手段と、
該情報送信装置に認証要求を発行して送るとともに、該情報送信装置から受信した認証要求に対する認証の判定を行う認証手段と、
該認証手段で認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該情報送信装置から受信した情報の暗号復号化処理を行う復号化手段と、
該情報送信装置への認証要求の送信もしくは該情報送信装置からの認証要求に対する応答の送信に対する該情報送信装置からの受信確認の到達までの時間を計測する時間計測手段とを有し、
該時間計測手段での計測結果が所定の値を超えた場合には、該情報送信装置からの情報受信を行わないことを特徴とする情報受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は映像音声等のコンテンツ等の情報を、ネットワークを介して送受信するのに際して、伝送されるコンテンツの著作権を保護するのに好適な送信装置、受信装置およびコンテンツ伝送方法に関するものである。
【０００２】
【従来の技術】
パーソナルコンピュータ（以下ＰＣと記す）の演算速度や記憶容量など処理能力の発展に伴い、ＰＣに内蔵されるハードディスクドライブ（以下ＨＤＤと記す）も大容量化が進んでいる。こうした状況のもとで最近では一般の家庭で利用されるようなランクのＰＣにおいてもＨＤＤを利用してＴＶ放送番組を録画し、これをＰＣのディスプレイで視聴を行うといった使い方ができるようになってきた。
またその一方では大容量ＨＤＤの低価格化により、家庭用の録画装置としてもＨＤＤを内蔵してこれに映像音声情報をデジタル記録するようなＨＤＤ録画装置が登場してきており、ディスクを録画媒体として使うことに拠る使い勝手の良さが着目されている。
上記したようなＨＤＤを利用した録画装置やＰＣなどでは映像音声情報は装置内に固定されたＨＤＤに録画されているため、家の中の他の部屋で録画した番組を視聴しようとするような場合には装置自体を持ち運ぶしかなく、ＶＴＲなど取替え可能な媒体を利用する録画再生装置を複数備えて行えるような、媒体レベルでの映像音声情報の持ち運びは実現が難しかった。

【０００３】
そこで、このような録画装置に有線あるいは無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）のインターフェースを搭載して、ネットワークを介して他のＰＣあるいは受信装置に送信することにより、宅内のどこでも録画された映像音声情報を視聴できるようにすることが考えられている。
【０００４】
一方コンテンツ等の情報の著作権保護のため、デジタルＡＶ機器に取り入コピープロテクトの方法の一例として例えばＩＥＥＥ１３９４バス上でのコピープロテクト方法を定めたＤｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ（ＤＴＣＰ）方式がある。（〔非特許文献１〕に記載）
そして、装置間、あるいはネットワーク間での著作権保護のためのコピープロテクトを実現するための技術がいくつか開示されている。例えば〔特許文献１〕、〔特許文献２〕に開示されている。
【０００５】
【特許文献１】
特開２０００－２８７１９２号公報
【特許文献２】
特開２００１－３５８７０６号公報
【非特許文献１】
Ｈｉｔａｃｈｉ，Ｌｔｄ．他、５Ｃ Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ Ｗｈｉｔｅ Ｐａｐｅｒ
【０００６】
【発明が解決しようとする課題】
上記した従来の技術で、家庭用の録画装置に有線あるいは無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）のインターフェースを搭載して、コンテンツをネットワークを介して他のＰＣあるいは受信装置に送信して、宅内のどこでも録画された映像音声情報を視聴できるようにする場合従来は、著作権を保護すべき映像音声情報（以下コンテンツとして説明する）の著作権保護については配慮がされておらず、ＨＤＤに録画されている映像音声情報は、ＬＡＮを介して受信した他のＰＣにおいて更にＨＤＤに保存することが可能であり、扱える映像音声情報はコピーが自由に行なえる「コピー制限なし」のコンテンツでなければならなかった。
【０００７】
一般にデジタル録画されたコンテンツを上記のようにネットワーク等を介してある装置から他の装置へ伝送して記録を行なうような場合には伝送時のデータ品質の劣化が少なく、送信側の装置にあるコンテンツと同じ品質のコピー（複製）が受信側で作成できるため、著作権を保護すべき映像および音声データ（以下コンテンツと呼ぶ）に対しては、個人的利用の範囲を逸脱したコンテンツの不正なコピー作成を防止できるような配慮が必要である。例えばデジタルＡＶ機器の間でコンテンツを送信する際には、コンテンツ送信装置側において暗号化を行ない、コンテンツ受信装置側との間で復号化のための情報の共有化を行なうことによって、送信先であるコンテンツ受信装置以外の機器によってコンテンツが正しく受信されて復号されない様にして、無制限なコピーの作成を防ぐコピープロテクトが実施されている。
【０００８】
このようなコピープロテクトの方法の一例としてデジタルＡＶ機器に取り入れられているものには、例えば〔非特許文献１〕に記載されているＤＴＣＰ方式がある。ＤＴＣＰ方式ではコンテンツを「コピー制限なし」「一回限りコピー可」「コピー禁止」に分類して管理し、録画装置では「コピー制限なし」「一回限りコピー可」のコンテンツだけを記録し、「一回限りコピー可」のコンテンツは一度記録した後は「コピー不可」として取り扱い、バス上では「コピー制限なし」のコンテンツを除いて送信側で暗号化処理を施して伝送を行なうことによって、無制限なコンテンツのコピーが行なえないようにしている。

【０００９】
有線あるいは無線のＬＡＮによるコンテンツ伝送においても、ＤＴＣＰ方式と同様な考え方により、著作権保護のためのコピープロテクトを実現するための技術がいくつか開示されている。例えば〔特許文献１〕は、ネットワーク上のデジタルコンテンツ流通のためのコピープロテクトの方式にＤＴＣＰと同様の手法を適用するための技術が開示されており、〔特許文献２〕にも同様にコンテンツを著作権保護のために暗号化して通信する装置間を構成するための技術が開示されている。
【００１０】
そして、これらはコンテンツを有線あるいは無線ＬＡＮを介して伝送する際には、送信側と受信側が同じ家の中に有るかどうかは考慮していない。むしろ、配信サーバからダウンロードを行うような場合には、送信側はプロバイダのサイトに有り、受信側は一般家庭などに有ることが普通である。
【００１１】
したがってＰＣのＨＤＤやＨＤＤを内蔵した録画装置でコンテンツを録画して、ここから宅内の他の装置にＬＡＮを介した伝送を行おうとする場合に上記の技術を適用したとしても、宅内のＬＡＮがインターネットに接続されているとインターネットを介して接続される他の宅内に置かれている受信装置でコンテンツを受信して表示することができ、しかもその範囲はインターネットに接続されていれば世界中のあらゆる場所に広がることになる。
このような状況では、例え上記したような技術でコピープロテクトを行おうとしても、録画装置の使用者がこの録画装置をインターネットからアクセス可能な状態にすることによって、上記のコピープロテクトを備えた受信装置であれば自由にコンテンツを受信して表示することができ、本来の著作権保護の目的である個人的利用の範囲を大きく逸脱することになってしまう。
【００１２】
本発明の目的は、宅内の有線または無線のＬＡＮを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成が個人的利用の範囲に制限することのできるコンテンツ或いは情報送信装置、受信装置およびコンテンツ伝送方法を提供することにある。
【００１３】
【課題を解決するための手段】
上記の課題を解決するため本発明では、ＬＡＮを介してコンテンツの送信を行うコンテンツ送信装置において、
ＬＡＮを介してデータの送受信を行うネットワーク通信処理手段と、
該ＬＡＮを介して接続されるコンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、
該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、
該認証手段で認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、
該コンテンツ受信装置への認証要求の送信もしくは該コンテンツ受信装置からの認証要求に対する応答の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を計測するタイマー手段を有し、
該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないようにする。
【００１４】
またこれに加えて、上記したコンテンツ送信装置において、
前記タイマー手段において計測した前記コンテンツ受信装置への認証要求の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間の計測結果が所定の値を超えた場

合には、前記認証手段において該コンテンツ受信装置の認証を不成功と判定する。
【００１５】
一方、上記の課題を解決するため本発明では、ＬＡＮを介してコンテンツの受信を行うコンテンツ受信装置において、
ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該ネットワークを介して接続されるコンテンツ送信装置から受信するコンテンツを該ネットワーク通信手段から受け取るコンテンツ受信処理手段と、
該コンテンツ送信装置に認証要求を発行して送るとともに、該コンテンツ送信装置から受信した認証要求に対する認証の判定を行うと認証手段と、
該認証手段で認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該コンテンツ送信装置から受信したコンテンツの暗号復号化処理を行う復号化手段と、
該コンテンツ送信装置への認証要求の送信もしくは該コンテンツ送信装置からの認証要求に対する応答の送信に対する該コンテンツ送信装置からの受信確認の到達までの時間を計測するタイマー手段を有し、
該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ送信装置からのコンテンツ受信を行わないようにする。
【００１６】
また、これに加えて、上記したコンテンツ受信装置において、
前記タイマー手段において計測した前記コンテンツ送信装置への認証要求の送信に対する該コンテンツ送信装置からの受信確認の到達までの時間の計測結果が所定の値を超えた場合には、前記認証手段において該コンテンツ送信装置の認証を不成功と判定する。
【００１７】
更に、上記の課題を解決するため本発明では、
ネットワークを介したコンテンツ送信装置とコンテンツ受信装置との間のコンテンツ伝送方法において、
該コンテンツ送信装置には、
ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該コンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、
該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、
該認証手段で認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、
該コンテンツ受信装置への認証要求の送信もしくは該コンテンツ受信装置からの認証要求に対する応答の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を計測するタイマー手段を設け、
該コンテンツ受信装置には、
ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該コンテンツ送信装置から受信するコンテンツを該ネットワーク通信手段から受け取るコンテンツ受信処理手段と、
該コンテンツ送信装置に認証要求を発行して送るとともに、該コンテンツ送信装置から受信した認証要求に対する認証の判定を行うと認証手段と、
該認証手段で認証処理を実行して得られる情報を元に生成した鍵情報によって鍵情報を生成し、該鍵情報により該コンテンツ送信装置から受信したコンテンツの暗号復号化処理を行う復号化手段と、
該コンテンツ送信装置への認証要求の送信もしくは該コンテンツ送信装置からの認証要求に対する応答の送信に対する該コンテンツ送信装置からの受信確認の到達までの時間を計測するタイマー手段を有し、

該コンテンツ送信装置の有する該タイマー手段での計測結果もしくは該コンテンツ受信装置の有する該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ送信装置から該コンテンツ受信装置へのコンテンツ送出を行わないようにする。

【００１８】

【発明の実施の形態】

以下本発明の実施の形態について説明する。

図１は本発明の一実施形態であるコンテンツ送信装置１００およびコンテンツ受信装置２００の構成を示したものであり、コンテンツ送信装置１００とコンテンツ受信装置２００とは互いにＬＡＮを介して接続されている。

【００１９】

コンテンツ送信装置１００はＬＡＮを介してコンテンツ受信装置２００に送信するコンテンツを送り出すコンテンツ送信回路１０１、コンテンツ送信回路１０１の出力するコンテンツを暗号化する暗号化回路１０２、暗号化回路１０２の出力および認証回路１０４の入出力をＬＡＮを介して他の装置とやり取りするネットワーク通信処理回路１０３、ＬＡＮ上に接続される他の装置との間で情報をやり取りして装置間の相互認証を行なう認証回路１０４、認証回路１０４での処理に必要な情報を蓄える不揮発メモリ１０５、認証回路１０４の出力する情報に基づき暗号化回路１０２でのコンテンツ暗号化のために必要な鍵情報を生成する鍵生成回路１０６、認証回路１０４で相互認証に成功した回数を計測して保持するカウンタ回路１０７、認証回路１０４が発生する認証要求などの情報を他の装置に送信してから該情報に対する受信確認が到達するまでの時間を測定するタイマー回路１０８から成る。コンテンツ送信回路１０１の送信するコンテンツは特定の種類の物に限定されることはなく、例えばＴＶ放送から受信している番組の映像および音声データや、ＨＤＤやＤＶＤなどのディスクまたはテープなどの記録媒体から再生している映像および音声データなどの全ての種類の情報が適用できる。

【００２０】

図１においては放送受信のためのチューナや録画再生のための手段およびネットワークでの伝送に先立ち必要となるデータ圧縮処理回路などについては図面上では省略している。送信しようとするコンテンツの種類に応じてこれらの手段を適宜構成に加えればよい。コンテンツ送信回路１０１から送信されるコンテンツにはその取り扱い方を示す「コピー制限なし」「一回限りコピー可」「コピー禁止」「コピー不可」の識別コードを付してコンテンツ受信装置に送信される、

コンテンツ受信装置２００はＬＡＮを介して送られてきたコンテンツを受信するコンテンツ受信回路２０１、コンテンツ送信装置１００の暗号化回路１０２で暗号化されたコンテンツをネットワーク通信処理回路２０３から受け取り復号化してコンテンツ受信回路２０１に出力する復号化回路２０２、他の装置との間でネットワークを介して復号化回路２０２への入力および認証回路２０４の入出力をやりとりするネットワーク通信処理回路２０３、他の装置との間で情報をやり取りして装置間の相互認証を行う認証回路２０４、認証回路２０４での処理に必要な情報を蓄える不揮発メモリ２０５、認証回路２０４の出力する情報に基づき復号化回路２０２でのコンテンツ復号化のために必要な鍵を生成する鍵生成回路２０６、認証回路２０４から他の装置に認証要求などの情報を送信してから該情報に対する受信確認が到達するまでの時間を測定するタイマー回路２０８から成る。コンテンツ受信回路２０１の出力である映像および音声データはディスプレイ装置によって表示されたりディスクやテープなどの記録媒体に記録されたりその利用形態は様々であり、本発明はその形態が特定の物に限定されることはない。

図１ではディスプレイや録画の手段や受信したデータ圧縮処理済みコンテンツの伸張復元手段は省略しているが、受信したコンテンツの利用形態に応じ適宜構成に加えればよい。なお、受信したコンテンツは該コンテンツと共に送信される「コピー制限なし」「一回限りコピー可」「コピー禁止」「コピー不可」の識別コードに従って処理され、「コピー制限なし」「一回限りコピー可」のコンテンツ記録媒体への記録が可能であり、「一回限りコピー可」のコンテンツを記録した場合にはそれ以後該コンテンツは「コピー不可」とし

て取り扱う。

【００２１】

図２はコンテンツ送信装置１００およびコンテンツ受信装置２００を含むＬＡＮの構成例を示したものである。１台のコンテンツ送信装置１００と２台のコンテンツ受信装置２００ａ、２００ｂは有線ＬＡＮのケーブルによりネットワークハブ装置４００にそれぞれ接続され、ネットワークハブ装置４００はさらにルータ３００に接続される。ルータ３００は図示しないモデムあるいは光電変換器などを介して、もしくはルータに内蔵されるモデムあるいは光電変換器によりインターネットに接続される。

【００２２】

インターネットへの接続形態はＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ Ｄｉｇｉｔａｌ Ｓｕｂｓｃｒｉｂｅｒ ｌｉｎｅ）や光ファイバーなどの高速アクセス回線やＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅｓ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋ）、アナログ電話回線、携帯電話などの移動体通信網などその種類を問わない。図２中の点線はコンテンツが送受信される装置とその方向を示している。

【００２３】

図２のＬＡＮの構成は一例を示したに過ぎず、コンテンツ受信装置２００は３台以上接続されていてもよい。またコンテンツ送信装置も２台以上接続されていてもよく、その場合にはそれぞれのコンテンツ送信装置から同時に異なるコンテンツをコンテンツ受信装置に対して、ＬＡＮの帯域の許す限り送信することが可能である。なお、本発明における必要最低限の構成はコンテンツ送信装置およびコンテンツ受信装置各１台がＬＡＮに接続された状態である。

【００２４】

図２に示すＬＡＮにおいてはネットワークプロトコルとして標準のＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）を使用し、上位のトランスポートプロトコルにはＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）およびＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）を用いる。コンテンツの伝送には更に上位のアプリケーションプロトコル、例えばＲＴＰ（Ｒｅａｌ－ｔｉｍｅ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ）やＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）等が使用される。なお、ＩＰにはバージョンの違いとしてＩＰｖ４とＩＰｖ６が有るが、本発明はそのどちらかに限定される物ではない。

【００２５】

コンテンツ送信装置１００、およびコンテンツ受信装置２００ａ、ｂ、ルータ３００はそれぞれＬＡＮ上で自身を識別するＩＰアドレスを所有する。また各々のネットワーク通信処理回路のインターフェース部には４８ビットのＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）アドレスが予め製造時に与えられている。各装置へのＩＰアドレスの設定は、従来よりネットワークにおけるアドレスの自動設定に広く採用されているＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）により、例えばルータ３００をＤＨＣＰサーバとして動作させ、ここから各装置のＩＰアドレスを割り振るようにすれば良い。なお、ＩＰｖ６を用いる場合にはステートレス自動設定と呼ばれる方法によりルータ３００のＩＰアドレスの上位６４ｂｉｔとＭＡＣアドレスから各装置が自身のＩＰアドレスを定めることも可能である。

【００２６】

図３はコンテンツ送信装置１００とコンテンツ受信装置２００によるコンテンツ送受信の際の手順の一例を示したものである。左側がコンテンツ送信装置１００を、右側がコンテンツ受信装置２００をそれぞれ表しており、両者の間の情報の送受信のタイミングと方向を矢印により示している。

コンテンツの送信に先立ちコンテンツ送信装置１００とコンテンツ受信装置２００との間で互いに相手方の装置の認証を行い、相手方の装置が著作権保護の規則に則って正しく製造された装置であることを確認してからコンテンツの伝送を行うようにする。認証のための情報の送受信にはプロトコルとしてＴＣＰを用い、相手方の装置への認証要求とこれに

対する認証応答等の各種情報が送信されるとこれに対する受信確認が相手方の装置から返送され、これにより伝送エラーの検知が可能な通信路が確保される。なお、図３においてはＴＣＰによるコネクション確立および廃棄のためのデータの送受信については省略してある。

【００２７】

始めにコンテンツ受信装置２００の側から認証要求を作成する。認証要求には特定の認証機関により生成されコンテンツ受信装置２００の不揮発メモリ２０５に保持される装置固有の公開鍵と該公開鍵に対する証書を付してコンテンツ送信装置１００に送る。公開鍵および証書は不揮発メモリ２０５にコンテンツ受信装置２００の製造時に予め記憶させておく。認証要求を受け取りその受信確認をコンテンツ受信装置２００に送るとコンテンツ送信装置１００は自分の側からの認証要求を作成し、コンテンツ受信装置の場合と同様に認証機関が発行したコンテンツ送信装置１００の固有の公開鍵とその証書を付してコンテンツ受信装置側２００に送り、タイマー回路１０８をスタートさせ認証要求に対する受信確認がコンテンツ受信装置から受信されるまでの時間Ｔ１を測定する。

【００２８】

その一方でコンテンツ送信装置１００は所定の公開鍵署名アルゴリズムに基づきコンテンツ受信装置２００の認証を行う。カウンタ１０７の数値をチェックし、現在値が所定の値を超えている場合には認証は不成功とし、認証に成功した場合にはカウンタ１０７の値を１だけ増加させる。また、タイマー１０８での計測値Ｔ１が所定の値を超えている場合には認証を不成功と判定する。認証が成功した場合には認証応答を発行してコンテンツ受信装置２００に送信する。同様にしてコンテンツ受信装置２００の側でもコンテンツ送信装置１００からの認証要求を受け取った後認証を行い、成功した場合には認証応答を発行してコンテンツ送信装置１００に送信する。以上のようして相互に認証に成功すると互いに共通の認証鍵が生成されて共有化される。認証鍵の生成にはＤｉｆｆｉｅ－Ｈｅｌｌｍａｎなど周知の鍵交換アルゴリズムを利用すれば良い。

【００２９】

認証鍵の共有が完了するとコンテンツ送信装置１００は交換鍵と乱数を生成し、交換鍵と乱数をそれぞれ認証鍵により暗号化してコンテンツ受信装置２００に送る。なお、図３では交換鍵と乱数を別々にコンテンツ送信装置１００からコンテンツ受信装置２００に送信しているがこれらをまとめて送るようにしてもよい。コンテンツ受信装置２００では認証鍵を用いてコンテンツ送信装置１００から送信された交換鍵を復号し、同様に受信して復号した乱数と共に保有する。続いてコンテンツ送信装置１００およびコンテンツ受信装置２００各々の側で交換鍵と乱数を用いて予め定められた計算アルゴリズムに従い共通鍵を生成する。このようにして得た共通鍵によってコンテンツ送信装置１００からコンテンツを暗号化して送信し、コンテンツ受信装置２００では復号化されたコンテンツを受信することができるようになる。

【００３０】

実際にコンテンツの送信を始めるにあたっては例えば図３に示すようにコンテンツ受信装置２００からコンテンツ送信要求を送り、これをきっかけとしてコンテンツの送信を行うようにする。コンテンツの送信が完了したらコンテンツ送信装置１００より送信完了を知らせても良いし、逆にコンテンツ受信装置２００側から送信終了を要求するようにしても良い。また、予め送信するコンテンツのデータ量がわかっている場合には特にどちらかの側から送信完了を知らせたり要求したりする必要は無い。必要なコンテンツの送信がすべて完了した後には、コンテンツ送信装置１００は認証鍵、交換鍵、乱数、共通鍵を破棄する。コンテンツ受信装置２００においてもコンテンツの受信が完了したら認証鍵、交換鍵、乱数、共通鍵を破棄するようにし、再度コンテンツの受信を行おうとする際には新たに認証要求から行えば良いが、コンテンツ送信装置１００が他のコンテンツ受信装置にコンテンツを送信していて以前の鍵が再度利用できる場合には、コンテンツ受信装置２００からコンテンツ送信装置１００に現在の鍵の情報を問い合わせた上で以前の鍵を再利用してもよい。

【００３１】
コンテンツ送信装置１００からコンテンツ受信装置２００にコンテンツを送信するのに使用するプロトコルは特定のものに限定されることはなく、先にも記した通りＲＴＰ、ＨＴＴＰ、ｆｔｐ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）等を用いることが可能である。コンテンツの伝送に際しては各転送プロトコルにおけるペイロード部分に共通鍵を用いて予め決められたアルゴリズムにより暗号化したコンテンツを収容して送信すれば良い。暗号化アルゴリズムとしては例えばＤＴＣＰにおいて採用されているＭ６暗号などを利用できる。
【００３２】
以上のようにして、図１に示したコンテンツ送信装置１００とコンテンツ受信装置２００との間で共通の暗号化用の鍵を用いて暗号化したコンテンツを送受信するので、ＬＡＮ上の他の装置によってコンテンツが受信されたとしても正しく復号化することができず、コンテンツが使用者のもとで不正に複製されるのを防止することができる。
【００３３】
図２に示すように一度に２台以上のコンテンツ受信装置によりコンテンツを受信することも可能である。この場合には各々のコンテンツ受信装置とコンテンツ送信装置との間で図３に示す手順に従い相互に認証を行った後にコンテンツの伝送を行えばよい。このときに１台のコンテンツ送信装置が認証をおこなったコンテンツ受信装置の数はカウンタ１０７でカウントされるので、コンテンツ送信装置の側でコンテンツ受信装置の認証を行う際に台数の上限を定めることによって、コンテンツ受信装置を同時に複数台用いて作成できるコンテンツの複製の数を制限することが可能になる。コンテンツ受信装置の台数の上限に関しては例えばＩＥＥＥ１３９４を用いて一度に接続可能なコンテンツ受信装置の上限である６２台かあるいはそれよりも小さな値とすればよい。
【００３４】
また、コンテンツ受信装置２００がインターネットを介して使用者の家とは異なる他の家に置かれているような場合には、コンテンツ送信装置からの認証要求およびこれに対する受信確認が、広域ネットワークおよびルータ３００を介して送受信されるため、宅内における送受信よりも往復の所要時間が増加する。そこで、Ｔ１の測定結果に対して認証を成功と判断するための上限値を適当な値、一例として１０ミリ秒など、に定めてやれば、コンテンツの伝送可能な範囲を使用者の宅内にとどめるような制限も可能になる。
【００３５】
コンテンツ送信装置１００における認証の判定に上記した図３におけるＴ１の測定結果を加味するのに加え、図３内に示すコンテンツ送信装置１００からの認証応答に対するコンテンツ受信装置２００の受信確認が到達するまでの時間Ｔ２をタイマー１０８で測定し、その結果が前記した所定の値を超えた場合には以後の交換鍵および乱数の送信を行わずにコンテンツ受信装置２００へのコンテンツの送信を行わないようにすることもできる。あるいはコンテンツ送信装置１００においてコンテンツ受信装置２００の認証を行う際にはＴ１の測定結果を加味せずに判定し、Ｔ１およびＴ２両方の測定結果をもとに交換鍵および乱数を送信するか否かの判定を行うようにしてもよい。
【００３６】
コンテンツ受信装置２００の側でも同様にして認証要求に対するコンテンツ送信装置１００からの受信確認が到達するまでの時間Ｔ３を測定し、その結果が前記した所定の値を超えている場合にはコンテンツ送信装置１００のからの認証要求に対して不成功の判定を下すようにしてもよい。これによりコンテンツ受信装置２００の側でも宅外からコンテンツを受信することを抑止することが可能になり、コンテンツの個人的利用の範囲を超えるようなコンテンツの伝送を防止できる。
あるいはまた、コンテンツ受信装置２００におけるＴ３の計測結果をコンテンツ送信装置１００からの認証要求に対する認証応答の送信時に含めて送り返し、コンテンツ送信装置の側でコンテンツの伝送を行うか否かの判定に供することもできる。
【００３７】

更には認証要求およびその結果に対する認証応答を送信する際のＴＣＰパケットを送信する際やコンテンツの伝送を行うＴＣＰパケットもしくはＵＤＰデータグラムを格納して送信されるＩＰパケットの生存時間（ＴＴＬ、Ｔｉｍｅ　ＴｏＬｉｖｅ）を例えば３以下等の低い値にして送信し、認証要求がルータ３００を通過しないようにしてコンテンツの伝送が個人的な利用の範囲を超えないような制限を加えることもできる。

【００３８】

図４は本発明の第２の実施形態であるコンテンツ送信装置５００およびコンテンツ受信装置６００の構成を示している。図４に示すコンテンツ送信装置５００およびコンテンツ受信装置６００において第１図のコンテンツ送信装置１００およびコンテンツ受信装置２００と異なる点は無線ＬＡＮを使ってコンテンツの伝送を行う点にあり、ＬＡＮとの接続に無線ネットワーク通信処理回路５０３および６０３を用い、ＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）暗号処理回路５０９および６０９を備えている点にある。ＷＥＰは無線ＬＡＮにおけるセキュリティ保護の目的で標準的に用いられている周知の暗号化方式であり、送信装置と受信装置の間でセキュリティ保護がなされた通信をユーザの管理下で実現することができる。

【００３９】

図５は図４に示したコンテンツ送信装置５００とコンテンツ受信装置６００を用いた宅内のネットワークの構成の一例を示している。図５においてデータ送信装置５００と２台のデータ受信装置６００ａ、６００ｂが無線アクセスポイント７００により無線ＬＡＮで接続される。無線ＬＡＮアクセスポイント７００はさらにルータ３００に接続され、ルータ３００は図２に示したルータ３００と同様にしてインターネットに接続される。

【００４０】

図４に示すコンテンツ送信装置５００とコンテンツ受信装置６００との間で相互認証とそれに続くコンテンツの伝送を行おうとする場合には、認証回路５０４および６０４によりＷＥＰ暗号処理回路５０９および６０９においてＷＥＰ処理が施されているかどうかをチェックする。そしてＷＥＰ処理が使われていなければ、相互認証とそれに続くコンテンツの伝送を行わないようにするか、もしくは使用者にＷＥＰ処理を起動させるように促す表示を行うなどの必要な処理をおこなうようにする。以上のようにして、無線ＬＡＮを用いてコンテンツの伝送を行う際には必ずＷＥＰ処理が施された状態となるようにする。この結果、コンテンツ送信装置５００およびコンテンツ受信装置６００の使用者が意識しないところで無線ＬＡＮを介して他のデータ受信装置が接続されてコンテンツの不正なコピーが行われてしまうのを防止する。

【００４１】

上記した以外の点に関しては図１から図３までに示された本発明の第１の実施形態であるコンテンツ送信装置およびコンテンツ受信装置により実施されるコンテンツの伝送方法と全く同様にして、コンテンツの不正な複製の作成を抑止して著作権の保護を行うことができ、その際に個人の利用範囲を逸脱したコンテンツの伝送が行なわれないようにすることができる。

【００４２】

以上で説明した本発明の実施の形態では有線ＬＡＮを用いる場合と無線ＬＡＮを用いる場合とを別々に説明したが、これらを同時に使用して家庭内のＬＡＮを構築することも可能であり、その際にも本発明を適用することが可能である。図６は有線と無線を両方用いて構成したＬＡＮにおいて本発明の実施形態であるコンテンツ送信装置とコンテンツ受信装置を使用する場合の構成を示した物である。

【００４３】

図６においてコンテンツ送信装置１００、コンテンツ受信装置２００ａ、２００ｂはネットワークハブ装置４００を介して互いに接続され、更に無線アクセスポイント７００もネットワークハブ装置４００に接続される。無線アクセスポイント７００にはコンテンツ送信装置５００、コンテンツ受信装置６００ａ，ｂが無線ＬＡＮによって接続されている。またネットワークハブ装置４００はルータ３００に接続されており、これにより宅内のＬ

ＡＮはインターネットに接続される。

【００４４】

図６の中で細い矢印の点線で示したのはコンテンツの伝送方向であり、各々のコンテンツ送信装置およびコンテンツ受信装置は相手方が有線ＬＡＮで接続されているのか無線ＬＡＮで接続されているのかを意識することなく、互いの間でコンテンツの伝送を行うことができる。その際の伝送手順は図３を用いて説明したのと全く同様でよい。また、無線ＬＡＮを用いるコンテンツ送信装置５００およびコンテンツ受信装置６００ａ、ｂにおいては先に説明したのと同様にＷＥＰの稼動をチェックしてから相互の認証およびコンテンツの伝送を行うようにすればよい。この場合でも有線あるいは無線のＬＡＮを単独で構成した場合と同様にコンテンツ伝送の際の不正な複製の作成を防止することができ、しかもコンテンツ伝送を個人的利用の範囲にとどめることができる。

【００４５】

以上の説明ではネットワークを介して伝送する対象を映像情報等のコンテンツとして説明したが、映像情報等以外の種類の情報についても同様であり、これらの情報を扱う情報送信装置、情報受信装置についても、本発明を実施できる。

【００４６】

また、以上説明した本発明の実施の形態における、認証回路、鍵生成回路、暗号化回路、復号化回路、カウンタ回路、タイマー回路等はハードウェアによる実現に限定される物ではなく、これらのうちの一部ないしは全てをマイクロプロセッサとその上で実行されるソフトウェア処置によって実現しても良く、その際でも本発明の効果を発揮する上での違いはない。

【００４７】

なおここまでの説明の都合上、コンテンツ送信装置とコンテンツ受信装置を別々の物としているが、コンテンツをディスクあるいはテープなどの記録媒体上に記録再生を行う装置においては、コンテンツ送信装置とコンテンツ受信装置の両方を兼ね備えるようにして構成してもよく、その際には認証回路や不揮発メモリなどを共用化することができる。

【００４８】

以上説明したように、本発明では宅内の有線または無線のＬＡＮを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成が個人的利用の範囲に制限することのできるコンテンツ送信装置、受信装置およびコンテンツ伝送方法を提供することができる。

【００４９】

【発明の効果】

本発明によれば、宅内の有線または無線のＬＡＮを利用したコンテンツ送信装置、受信装置及びコンテンツ伝送の信頼性向上を図ることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態であるコンテンツ送信装置およびコンテンツ受信装置の構成を示すブロック図である。

【図２】本発明の第１の実施の形態であるコンテンツ送信装置およびコンテンツ受信装置により構成されるＬＡＮのブロック図である。

【図３】本発明の第１の実施の形態であるコンテンツ送信装置およびコンテンツ受信装置間でコンテンツの伝送を行うサイン手順を示すシーケンス図である。

【図４】本発明の第２の実施の形態であるコンテンツ送信装置およびコンテンツ受信装置の構成を示すブロック図である。

【図５】本発明の第２の実施の形態であるコンテンツ送信装置およびコンテンツ受信装置により構成されるＬＡＮのブロック図である。

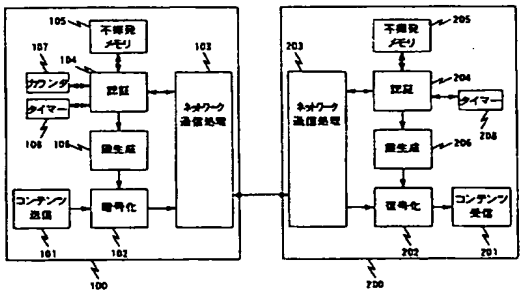
【図６】本発明の第１および第２の実施の形態であるコンテンツ送信装置およびコンテンツ受信装置により構成されるＬＡＮのブロック図である。

【符号の説明】

１００、５００・・コンテンツ送信装置
１０１、５０１・・・コンテンツ送信回路
１０２、５０２・・・暗号化回路
１０３、５０３・・・ネットワーク通信処理回路
１０４、５０４・・・認証回路
１０６、５０６・・・鍵生成回路
１０７、５０７・・・カウンタ回路
１０８、５０８・・・タイマー回路
２００、６００・・・コンテンツ受信装置
２０１、６０１・・・コンテンツ受信回路
２０２、６０２・・・復号化回路
２０４、６０４・・・認証回路
２０６、６０６・・・鍵生成回路
２０８、６０８・・・タイマー回路

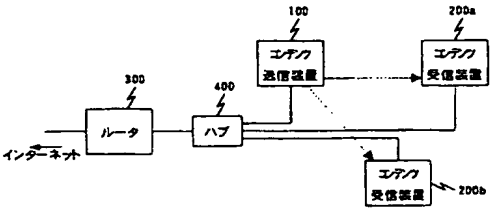
【図１】

図 1



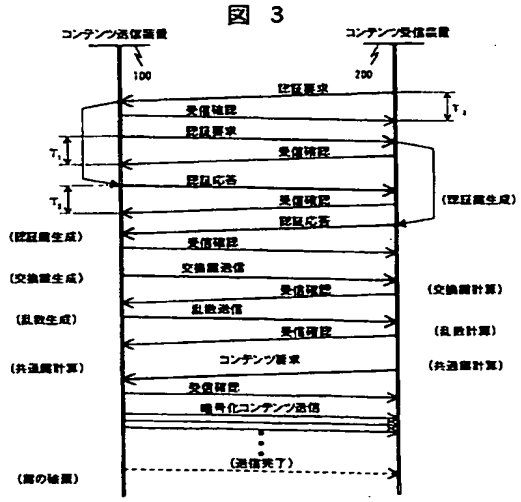
【図２】

図 2



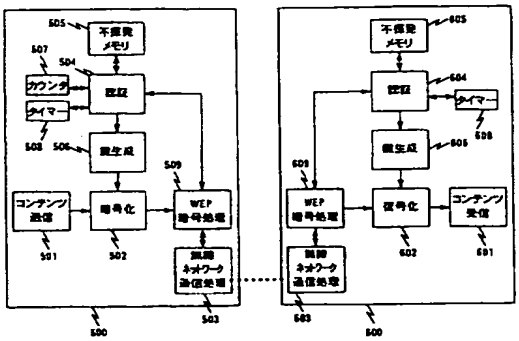
【図３】

図 3



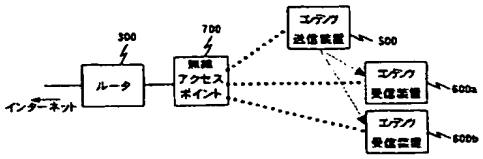
【図４】

図 4



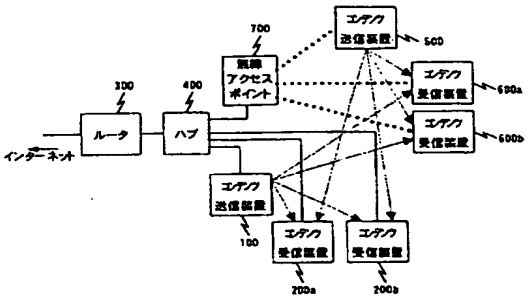
【図５】

図 5



【図６】

図 6



フロントページの続き

(72)発明者　岡本　宏夫
神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立製作所デジタルメディア開発本部内

Ｆターム(参考) 5B085 AE04 AE09 AE29
5J104 EA23